

**COMMISSIONE PARLAMENTARE
DI VIGILANZA SULL'ANAGRAFE TRIBUTARIA**

RESOCONTO STENOGRAFICO

INDAGINE CONOSCITIVA

29.

SEDUTA DI GIOVEDÌ 16 LUGLIO 2015

PRESIDENZA DEL PRESIDENTE GIACOMO ANTONIO PORTAS

INDICE

	PAG.
Sulla pubblicità dei lavori:	
Portas Giacomo Antonio, <i>Presidente</i>	2
INDAGINE CONOSCITIVA SULL'ANAGRAFE TRIBUTARIA NELLA PROSPETTIVA DI UNA RAZIONALIZZAZIONE DELLE BANCHE DATI PUBBLICHE IN MATERIA ECONOMICA E FINANZIARIA. POTENZIALITÀ E CRITICITÀ DEL SISTEMA NEL CONTRASTO ALL'EVAZIONE FISCALE	
Audizione del presidente e amministratore delegato della SOGEI S.p.A., Cristiano Cannarsa:	
Portas Giacomo Antonio, <i>Presidente</i>	2, 7, 8
Bignami Laura (Misto-Movimento X)	6
Cannarsa Cristiano, <i>presidente e amministratore delegato di SOGEI S.p.A.</i>	2, 6, 8
Pagano Alessandro (AP)	6

PRESIDENZA DEL PRESIDENTE
GIACOMO ANTONIO PORTAS

La seduta comincia alle 8.40.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta odierna sarà assicurata mediante l'attivazione del sistema audiovisivo a circuito chiuso e la trasmissione diretta sulla *web-tv* della Camera dei deputati e, successivamente, sul canale satellitare della Camera dei deputati.

(Così rimane stabilito).

Audizione del presidente e amministratore delegato della SOGEI S.p.A., Cristiano Cannarsa.

PRESIDENTE. L'ordine del giorno reca l'audizione del presidente e amministratore delegato della SOGEI S.p.A., ingegner Cristiano Cannarsa che, anche a nome dei colleghi, ringrazio per aver accolto l'invito della Commissione. È inoltre presente la dottoressa Anna Scafuri, responsabile delle relazioni istituzionali e comunicazione, che ringrazio per la presenza.

L'audizione si inquadra nell'ambito dell'indagine conoscitiva sull'anagrafe tributaria nella prospettiva di una razionalizzazione delle banche dati pubbliche in materia economica e finanziaria. Potenzialità e criticità del sistema nel contrasto all'evasione fiscale.

Do la parola all'ingegner Cannarsa, con riserva per me e per i colleghi di rivolgervi, al termine del suo intervento, domande e richieste di chiarimenti.

CRISTIANO CANNARSA, *presidente e amministratore delegato della SOGEI S.p.A.* Raccolgo l'invito a cercare di contenere i tempi, perché la materia è ampia e la trattazione potrebbe essere troppo lunga.

Nell'ambito della sicurezza del sistema delle banche dati dell'Anagrafe tributaria, individuiamo tra le principali banche dati due recenti esempi di eccellenza dal punto di vista della gestione della sicurezza: mi riferisco all'anagrafe dei rapporti, cioè i conti correnti, e il 730 *web* precompilato.

La sicurezza si distingue in fisica, logica e quella concernente l'organizzazione per la protezione dei dati personali. In questo contesto, abbiamo conosciuto, in particolare negli ultimi mesi, una grande evoluzione a livello tecnologico e organizzativo. Abbiamo costituito il CERT Sogei e il SOC, *Security Operation Center*. Inoltre, visto il particolare momento, abbiamo anche svolto un caso di studio sull'*hacking team*, relativo cioè alla situazione verificatasi qualche giorno fa e che ha destato particolare preoccupazione per gli operatori del settore.

Abbiamo un sistema di tipo logistico, metodologico e tecnologico: per la logistica, in particolare, c'è un riferimento alla sicurezza fisica del nostro sito, classificata come un'infrastruttura critica a livello nazionale; sotto il profilo metodologico, l'attenzione è sulla *privacy* e sulla *security* in generale mentre, per il lato tecnologico, l'impegno è rivolto alla tracciabilità e al controllo degli accessi.

Operiamo in un sistema che, come sapete, è di *information governance*, vista la numerosità delle banche dati che gestiamo: il patrimonio informativo gestito da SOGEI è caratterizzato da più di cento banche dati — parliamo di banche dati strutturate, escluse quelle che contengono meta dati e quelle asservite da *business*

intelligence – e 84 domini. Gli utenti, che sono poi i titolari dei dati, sono i ministeri, in particolare le agenzie, e, a livello più ampio sono anche associazioni di categoria, cittadini, operatori economici, quindi le imprese, e i punti di commercializzazione dei monopoli, quindi la parte relativa ai giochi.

C'è una classificazione internazionale delle banche dati sulla base della RID (riservatezza, integrità e disponibilità), anche secondo la tipologia dei dati contenuti. Il livello di classificazione si traduce in misure di sicurezza idonee a garantire un grado di protezione adeguato, in funzione delle minacce derivanti dalla criticità del dato contenuto nella banca dati.

In questa rappresentazione, come vedete, i domini principali sono: il fisco, le dogane, i giochi, la sanità, il personale, il bilancio della finanza pubblica, la spesa della pubblica amministrazione e il catasto. Andando in senso orario, per il fisco abbiamo riportato alcuni numeri per dare un'idea. Nel 2014, abbiamo gestito 236 milioni di deleghe F24, con circa 550 milioni di codici tributo, che sono poi quelli che hanno portato nelle casse dello Stato circa 500 miliardi di entrate tributarie. In questo ambito ci sono anche gli avvisi, le comunicazioni, le dichiarazioni e i controlli che hanno portato circa 4,2 miliardi di incasso grazie al contrasto all'evasione.

Anche in ambito doganale, c'è un livello di flussi molto consistente, con circa 42 milioni di *file*, di dichiarazioni doganali, riguardanti tutti i transiti in entrata e in uscita delle merci da e verso i Paesi comunitari e anche extracomunitari.

Il settore dei giochi è molto particolare, a livello di sicurezza e *privacy*, perché è caratterizzato dai conti di gioco, aperti dai giocatori per poter esercitare il gioco *on line*. Di fatto, è come se fossero conti correnti, aperti nominativamente e caricati attraverso gli strumenti usuali: carte di credito e versamenti.

Per la sanità abbiamo riportato solo le ricette mediche. Nel 2014, vi sono state circa 800 milioni di ricette mediche elettroniche.

Vi è poi un punto particolare per il dominio del personale, dove vengono gestiti i cedolini delle buste paga: adesso siamo a circa 1.700.000 dipendenti pubblici, e questo è un ambito molto importante, a livello di gestione della sicurezza e della *privacy*.

Andrei velocemente sugli altri ambiti più strutturati, ossia quelli di bilancio e finanza pubblica, spese della pubblica amministrazione e catasto, che riguarda invece tutte le proprietà immobiliari, quindi fabbricati e terreni, dove poi vengono gestiti tutti i flussi di visure catastali e anche di interventi, quali accorpamenti e fusioni con specifiche applicazioni.

Un caso particolare di eccellenza è stato sicuramente, ed è, quello dell'anagrafe dei rapporti. Come sapete, nel 2012 è stato introdotto l'obbligo per le banche di comunicare a SOGEI tramite l'Agenzia delle entrate, i saldi di inizio e fine anno di tutti i conti correnti esistenti nelle banche italiane. Questa operazione è stata gestita con l'Autorità garante per la protezione dei dati personali in maniera molto accurata, sia per la parte relativa alla sicurezza dell'invio sia per quella relativa alla gestione dei dati, in ambito di consultazione e di indagine finanziaria. La consultazione è gestita da un servizio che consente l'accesso delle informazioni dall'Agenzia delle entrate, Guardia di finanza, Equitalia e poi anche dalla Direzione investigativa antimafia e dalle Procure della Repubblica. Sono state concluse convenzioni per gestire questi accessi, ognuno dei quali è profilato e tracciato. Capite bene, però, la potenza anche investigativa di questo strumento.

Il servizio di indagini finanziarie è a disposizione dell'Agenzia delle entrate, della Guardia di finanza, dell'Agenzia delle dogane e monopoli e consente l'interrogazione dell'archivio dei rapporti all'atto dell'autorizzazione da parte dell'organismo regionale.

Questi servizi hanno un perimetro di sicurezza certificato secondo lo standard 27.001 che definisce i requisiti per imple-

mentare, operare, monitorare e revisionare l'SGSI, il sistema di gestione della sicurezza delle informazioni.

Un altro caso particolarmente importante in tema di sicurezza è quello del 730 precompilato. La profilatura per l'accesso al 730 precompilato è un altro dominio riservato, perché ci sono informazioni su redditi, spese e consistenze patrimoniali. Lo stesso è stato trattato attraverso regole di gestione delle credenziali di autenticazione che prevedono un'identificazione univoca della persona fisica e un livello di autenticazione molto elevato; quindi *username* e *password*, che danno caratteristiche di robustezza del controllo molto elevate. Questo accesso è tracciato e dunque il codice del fruitore viene sempre registrato e conservato, dando così una garanzia anche in caso di rilevazione di abusi.

Dal punto di vista della sicurezza fisica, bisogna ridurre, a livello di organizzazione, le possibilità di accesso fisico ai sistemi. Il sistema, tramite perimetri concentrici di controllo, gestisce il livello di sicurezza, anche attraverso una collaborazione molto intensa con la Guardia di finanza che, mediante un protocollo d'intesa garantisce in materia di sicurezza fisica, garantisce il presidio h24, sette giorni su sette, della nostra sede di via Carucci 99. L'orario indicato nella documentazione dalle ore 6 alle ore 24 è relativo al personale Sogei; la GdF, che ha una caserma interna alla nostra struttura, effettua un presidio costante attraverso turnazioni che garantiscono il controllo h24 in tutti i punti dell'azienda; poi vi mostro anche come è strutturato. L'obiettivo è di ridurre la vulnerabilità, prevenire i rischi e dare una risposta tempestiva in caso di aggressioni, anche per un'analisi degli eventi. Abbiamo una infrastruttura di sicurezza fisica passiva, di controllo accessi fisici antintrusione e un'infrastruttura di video sorveglianza. La sede è protetta da un muro di cinta di cemento armato di circa 1.200 metri di lunghezza, di perimetro, in cemento armato, con un'altezza di circa 5 metri. Ha sistemi anti scavalco e antisfondamento, cioè

sensori che, in caso di scavalco o sfondamento, segnalano l'evento alla centrale operativa. Per gli accessi, oltre ad esserci il classico sistema di controllo, si prevede anche l'uso di RX e *metal detector*. Inoltre, c'è un sistema di videosorveglianza con circa 280 telecamere, sia a livello perimetrale, sia in azienda, nel rispetto delle regole: le telecamere in azienda, infatti, devono seguire norme per la *privacy*, con un tempo di conservazione di trenta giorni consentito grazie a una specifica approvazione del Garante, perché normalmente il tempo di conservazione è di sette giorni.

La sicurezza delle banche dati è strutturata con un *security operation center* che gestisce a livello centralizzato tutto il governo della sicurezza e che va dagli uffici dell'amministrazione finanziaria — abbiamo una rete composta da circa 1.300 uffici — ai CED dell'anagrafe tributaria, fino a tutte le aree esterne. Possiamo considerarne tre: l'area dei giochi, quindi le reti dei concessionari e le reti delle sale gioco; internet e il servizio pubblico di connettività. Come vedete, in ognuno di questi punti di interfaccia ci sono quei « muri » che sono i sistemi di *firewall* periferici e centrali che garantiscono la protezione del sistema Sogei.

La sicurezza logica fa riferimento al *security operation center*. C'è un controllo accessi, come avevo detto all'inizio della presentazione, sulle postazioni, sulle applicazioni interne, sugli amministratori di sistema e sui servizi telematici. Il controllo accessi garantisce, oltre alla profilatura per ciascuna utenza abilitata, anche il tracciamento di tutto quello che viene fatto da quell'utenza, ai fini del controllo a posteriori e dell'eventuale sanzione in sede civile e penale.

Per quanto riguarda il modello organizzativo, esso è basato su un delegato alla *privacy* incaricato dal vertice aziendale: si tratta di una figura prevista proprio dalla struttura del sistema di gestione della *privacy*. Quanto invece alle deleghe subordinate queste riguardano tutte le persone che trattano dati personali, che gestiscono gli ambiti tecnologici e i sistemi, ossia gli

amministratori di sistema. Ognuno di questi soggetti è profilato e tracciato, per cui ogni accesso è imputabile direttamente a una singola persona, ognuna delle quali ha una delega specifica, nominativa, che lo impegna ai sensi di legge.

Tra gli obiettivi generali, abbiamo quello della razionalizzazione dei costi e dei processi e la diffusione della digitalizzazione verso cittadini e imprese. Tali obiettivi devono necessariamente passare dalla razionalizzazione e l'interoperabilità delle banche dati delle strutture pubbliche. Questo tema è stato più volte menzionato in varie audizioni, ma è inevitabile che l'ampliamento dei servizi ai cittadini e alle imprese debba passare da una maggiore interoperabilità delle numerose banche dati presenti nella struttura pubblica, purtroppo molto spesso non strutturate. Ci sono approcci diversificati sull'evoluzione dei temi tecnologici della sicurezza, nel rispetto soprattutto dei diritti dei cittadini. C'è la necessità di garantire la sicurezza delle informazioni, ma allo stesso tempo di ampliare il numero di servizi a disposizione dei cittadini. Vedete bene come ci sia l'esigenza di un bilanciamento di queste due esigenze, una opposta all'altra.

Per quanto riguarda l'evoluzione del contesto tecnologico, abbiamo la necessità di proteggerci da attacchi cibernetici. Gli ambiti in cui ci stiamo cimentando attualmente sono soprattutto di livello tecnologico. Dobbiamo avere un livello elevato di sicurezza sulle piattaforme e l'introduzione tempestiva di nuove tecnologie di sicurezza. In prospettiva, dobbiamo anche evolvere il processo produttivo secondo le *best practice* a livello internazionale, in particolare dell'*open web application security project*. All'interno della nostra struttura, abbiamo un *team* dedicato di *ethical hackers*, che sono sostanzialmente persone che fanno *scouting* dell'attività di *hacking* svolta nel mondo dell'IT in generale, in particolare di internet, per essere sempre aggiornati su quello che sta succedendo e conoscere meglio i livelli di attacco.

Andando avanti, sul tema della sicurezza, uno dei punti di forza è la recente costituzione in Sogei del CERT, *Computer*

Emergency Response Team, costituito per cooperare con il CERT della pubblica amministrazione e che si avvale di un sistema di informazione che, oltre a essere quello interno al Ministero dell'economia e delle finanze e in particolare della Guardia di finanza, utilizza anche quello del CNAIPIC, il centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche, con il quale Sogei ha stipulato un accordo il 27 febbraio 2015, proprio per acquisire un flusso informativo anche da questo soggetto che ha una funzione di polo del crimine informatico.

Scambiamo informazioni anche il DIS, il dipartimento informazione di sicurezza della Presidenza del Consiglio dei ministri. Proprio tale dipartimento ha ormai definito il *cyber space* come parte integrante della vita reale e delle attività quotidiane dei cittadini, quindi non più qualcosa di astratto, ma uno spazio cui realmente siamo tutti in qualche modo vincolati e da cui siamo condizionati.

Quella che vi mostro è la struttura del CERT della pubblica amministrazione e del CERT Sogei. Come vedete, il CNAIPIC, il CERT della pubblica amministrazione, le fonti di *intelligence* e le varie *constituency* si collegano con il CERT Sogei e poi con altri CERT di altri clienti istituzionali, in particolare quelli di altre grandi imprese.

Passo a illustrare la gestione degli incidenti e gli *output* che il CERT Sogei fornisce. La gestione di incidenti interviene quando ci sono tentativi di attacco. Tenete conto che questi sono all'ordine del giorno: dall'inizio dell'anno abbiamo avuto circa un centinaio di tentativi di attacco, tutti gestiti e non andati a buon fine. Questo sistema di informazione sugli attacchi fornisce una base di storicizzazione di informazioni utile per l'analisi degli attacchi futuri e quindi vengono dati *output* a tutti i CERT della pubblica amministrazione ai CERT privati, al CNAIPIC e alle altre *constituency*.

Vengo al caso *Hacking team*, giusto per dare un piccolo resoconto. Come sapete, è un fatto che sta destando particolare preoccupazione, perché nella notte del 6 luglio scorso sono stati pubblicati 400

gigabyte di dati provenienti da *server* di *Hacking team*, una società italiana. In questa mole di dati c'era un elenco di clienti, di *mail*, di codici sorgente dei *software* di intercettazione. Si tratta di una società che opera nei *trojan* inseriti su *tablet* per le intercettazioni. Ha costituito particolare attenzione il fatto che fossero stati pubblicati i codici sorgente del *software*, che vuol dire di fatto il programma, quindi ora tutto il mondo in contatto con questa società è stato congelato per evitare che una volta noti i codici sorgente ciò potesse creare vulnerabilità alle strutture ad essi collegate. Sogei non ha mai avuto, diciamo, rapporti con questa società e quindi è indenne da qualsiasi contatto. Il CERT e il SOC di Sogei hanno monitorato l'evento e abbiamo analizzato anche tutti i dati pubblicati, per capire se contenesero informazioni relative alla nostra società: abbiamo trovato solo una mail relativa a una rassegna stampa che citava il nome di Sogei, ma niente di rilevante. Le analisi sono ovviamente ancora in corso. C'è un livello di attenzione molto elevato, ma a livello di sicurezza SOGEI non c'è stato alcun rischio.

Le risposte sulla sicurezza fisica le ho menzionate prima, citando i sistemi di sicurezza passiva, i sistemi antintrusione, *video intelligence*, quindi sistemi video che consentono anche il riconoscimento facciale; a tale riguardo, stiamo svolgendo un'analisi per introdurre anche queste nuove tecnologie nel sistema di videosorveglianza Sogei.

Quanto al *disaster recovery*, come sapete ne abbiamo uno sia a livello metropolitano, sia geografico, a oltre cento chilometri da Roma. Sono due strutture sottoposte a controllo, in particolare quello geografico si trova in una caserma della Guardia di finanza. La sicurezza per noi è un tema sul quale investire e al quale dedicare attenzione a livello di organizzazione e di risorse finanziarie, soprattutto alla luce di quello che sta succedendo. Ormai la vita delle persone è molto legata al *cyber space* e quindi è opportuno pre-

venire i rischi e dotarsi di un sistema di monitoraggio e controllo che consenta di attuare una prevenzione efficace.

LAURA BIGNAMI. La ringrazio anzitutto, perché è sempre molto chiaro e chiarificante.

Ero curiosa di sapere qualcosa su quei cento tentativi di attacchi *hacker* che ha menzionato. Immagino che abbiate fatto ricerche e dunque, per avere una statistica media, chiedo per quanti di questi siete riusciti a risalire alla fonte, con quale modalità e con l'aiuto di chi.

ALESSANDRO PAGANO. Vorrei intanto complimentarmi con l'ingegnere Cannarsa per la riconferma – è un dato ufficiale, visto che siamo in diretta – segno evidente del riconoscimento del lavoro fatto, perché altrimenti non ce ne sarebbe stato motivo. Detto ciò, volevo capire un attimo, forte di questa riconferma che certamente è la prova di una fiducia meritata sul campo, se esiste già una prospettiva di piano industriale e finanziario su cui state lavorando, che tenga conto ovviamente di tutti i cavalli di battaglia che hanno contraddistinto l'azione della sua gestione, ma devo dire anche il lavoro di questa Commissione, che ha sempre appoggiato pienamente il lavoro prezioso di Sogei.

CRISTIANO CANNARSA, *presidente e amministratore delegato della SOGEI S.p.A.* Rispondo alla prima domanda sul tema dei cento eventi. Gli eventi sono quotidiani. Non riguardano Sogei, ma coinvolgono in generale tutti i siti, in particolare quelli della pubblica amministrazione, che espongono servizi. Sogei, gestendo i siti internet di tutti i clienti, dall'Agenzia delle entrate alla Ragioneria generale, all'Agenzia delle dogane e monopolio, è il soggetto che monitora i tentativi di attacchi, comunque di lievissima entità, che mirano al rallentamento dell'efficienza dei siti attraverso, ad esempio, un numero di accessi elevati, per cui si cerca di paralizzare il sistema di accesso al sito. Sostanzialmente sono più disturbi, che attacchi di conte-

nuto dannoso. Non vanno a danneggiare, né a sottrarre in alcun modo dati, ma mirano solo a tentare di rallentare l'efficienza dell'amministrazione, sempre più legata al sito *web*. Quindi, se si rallenta il sito dell'Agenzia delle entrate, magari sotto scadenza delle dichiarazioni dei redditi, si crea un danno indiretto, ma ciò non si è mai verificato. Questi cento attacchi, non hanno avuto conseguenze. Il monitoraggio del *cyber space* che viene fatto è continuo. Ci sono ripetuti tentativi di approccio, che vanno sempre analizzati, perché tra questi tentativi prima o poi ce ne potrebbe essere uno con un contenuto più specifico.

Ringrazio l'onorevole Pagano per le sue parole. Ovviamente mi ha fatto molto piacere la riconferma, proprio per la continuità e il lavoro fatto in questi anni, devo dire con grande passione, in Sogei e con grande collaborazione con il Ministero dell'economia e con tutte le agenzie che sono state veramente sottoposte a un lavoro di intensità molto elevata.

Sul piano industriale citerei le parole dell'onorevole Baretta che qualche giorno fa, in un convegno, ha detto che in Italia serve un campione nazionale dell'informatica pubblica. Mi associo a questa sua affermazione, dicendo che Sogei sicuramente è il candidato principale in questo disegno. Ritengo che un campione nazionale in Italia serva, vista la dimensione delle aziende di IT negli altri Paesi. Giusto per dare qualche esempio, in Francia, l'azienda di più grandi dimensioni ha una consistenza di oltre 10.000 dipendenti — non facciamo nomi — e 14 miliardi di euro di fatturato e lo stesso vale per la Germania e per la Spagna. Stiamo parlando di soggetti che hanno una dimensione ormai globale e multinazionale, che operano non limitatamente all'ambito pubblico del Paese in cui risiedono. Penso che si debba trovare in Italia una posizione, proprio per garantire questa grande progettualità che c'è nell'IT pubblica, dove sicuramente la precompilata è stato quest'anno un esempio importante.

La progettualità secondo me è fondamentale. Avere grandi progetti aggrega

sicuramente l'offerta e la domanda, anche di nuove tecnologie. Quindi, nel momento in cui ci sono grandi progetti, ci sono anche grandi iniziative di aggregazione di soggetti che li sviluppano e l'offerta viene catalizzata su progetti importanti. Questa progettualità deve necessariamente, come ho detto prima, passare attraverso due pilastri fondamentali, la razionalizzazione delle infrastrutture e delle banche dati, insieme alla disponibilità a creare un campione nazionale che possa portare avanti questo progetto di IT pubblica in maniera adeguata. Ovviamente siamo non disponibili, ma di più, siamo i promotori di questa iniziativa e mi auguro che nei prossimi mesi possa prendere corpo.

PRESIDENTE. Mi aggiungo anch'io. Intanto complimenti per la conferma. In questi anni, il rapporto con Sogei è stato veramente forte, dal prossimo anno ancora di più, visto il pieno mandato che le hanno conferito. Penso di parlare a nome di tutta la Commissione nel dire che il punto nodale, per quanto riguarda questa Commissione, che in questi anni ha fatto qualcosina di buono insieme a voi, all'Agenzia delle entrate e alla Guardia di finanza, sarà, nei prossimi mesi — la avverto — un controllo sulla razionalizzazione delle banche dati. Chiedo se possibile — lo dico ai microfoni, per cui è registrato — avere nei prossimi mesi un prospetto del risparmio per la nazione che verrebbe dall'accorpamento di banche dati. Non voglio far nomi di tante altre agenzie dello Stato che tutto sommato sono doppiati di quello che fa Sogei. È vero, Sogei non è la società francese con 10.000 dipendenti, ma ne ha 2.150 e penso che possa davvero, al di là del risparmio economico per la nazione, razionalizzare e non perdere tutto questo tempo, come abbiamo fatto in questi anni, con società che forse avevano una ragione di esistere nel 1980, ma oggi Sogei può rappresentare tutte queste banche dati. Ricordo ancora l'audizione con Cottarelli sul risparmio che verrebbe per la nazione dall'accorpamento di banche dati; parlo di INPS e anche di altre società. Se questo è possi-

bile, come Commissione, chiederò il mandato ufficiale con una lettera ai componenti della Commissione, dal prossimo anno, per verificare ogni tre mesi l'andamento di questo progetto che penso sia importantissimo per l'Italia.

CRISTIANO CANNARSA, *presidente e amministratore delegato della SOGEI S.p.A.* Presidente, la ringrazio perché il lavoro di questi anni è stato fondamentale per creare le basi per quello di cui stiamo parlando. Penso che in Italia si debba fare sistema. Razionalizzare vuol dire capire innanzitutto cosa c'è e metterlo a sistema. In questa attività, oggi abbiamo anche un nuovo direttore dell'Agenzia per l'Italia digitale, Antonio Samaritani, con il quale stiamo già lavorando. Sto creando a livello organizzativo in Sogei una struttura che sarà deputata proprio al rapporto con l'Agenzia per l'Italia digitale. Metteremo a disposizione, all'interno di Sogei, competenze che possano aiutare e supportare Agenzia e Sogei in prima persona, nella mappatura e quindi nel progetto che diceva il presidente di banche dati oggi non interoperabili, dalla cui interoperabilità,

oltre a un grande risparmio, perché si ci sono forti efficienze a livello di economie di scala, si possono invece avere anche più servizi per i cittadini e per le imprese, che poi è quello che penso interessi tutti, perché la pubblica amministrazione si misura proprio dal livello di servizi che offre alla sua cittadinanza. Su questo siamo seriamente impegnati e ovviamente raccolgo l'invito a svolgere questa attività che porterò avanti con grande attenzione e che riporterò anche all'interno del Ministro dell'economia come una richiesta della Commissione.

PRESIDENTE. Nel ringraziare l'ingegner Cannarsa, dichiaro conclusa l'audizione.

La seduta termina alle 9.20.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE
DELLA CAMERA DEI DEPUTATI

DOTT. RENZO DICKMANN

*Licenziato per la stampa
il 6 agosto 2015.*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

